TI - METHOD AND DEVICE FOR VERIFYING A FILE

AB - The invention relates to a method and a device for verifying the authenticity and integrity of a file which has been received, or is to be transmitted from a computer (14) and which is furnished with a digital signature. For the verification process, said method accesses signals which are available at an interface (18) of the computer that is linked to an output device (16) for outputting the file furnished with the digital signature. A device (20) for carrying out the method comprises a circuit and a programme which are used to perform the verification in the device (20), in a manner which is logically separate from the central calculation unit of the computer (14). The device (20) is coupled to an interface (18) of the computer (14) that is linked to an output device (16), in such a way that it detects the signals used for the verification, in order to output the file furnished with the digital signature.

PN - WO0146785 A 20010628

AP - WO2000EP13122 20001221

OPD - 1999-12-21

PR - DE19991061838 19991221

PA - SCM MICROSYSTEMS GMBH (DE)HEINS KERSTEN W (DE)

IN - HEINS KERSTEN W (DE)

EC - G06F1/00N1V2

IC - G06F1/00

CT - EP0587375 A [A]; US5778071 A [A]; EP0722151 A [A]

TI - Verification of a file that is to be sent or received over a network, has a device separate from the host computer, capable of reading a signal from the peripheral interface, but independent of the host processor, to test the file

AB - WO200146785 NOVELTY - In order to verify file authenticity and integrity, the verification process accesses signals which are transferred over an interface (18) linking the computer to an output device (16) such as a monitor.

- DETAILED DESCRIPTION - An INDEPENDENT CLAIM is made for a device (20), for carrying out the verification process, which comprises a circuit and program that are entirely separate from the computer processor unit that can carry out the verification. The device is coupled to the output device so that the signals used for the testing are determined from the file with a digital signature. The device (20) includes an ASIC and can be mounted on the main-board, on an expansion card or on a chip card terminal. The output device (16) can be a printer or a terminal. The device includes a true false display to indicate clearly to a user the state of the file.
- USE - Method and device for verifying a file that is to be transmitted from or received by a computer over a network.
- ADVANTAGE - Use of an external verification device that is totally independent of the computer processor means that no virus effects can interfere with the

encryption or decryption processes.

- DESCRIPTION OF DRAWING(S) - (Drawing includes non-English language text). Figure shows a schematic flow diagram for testing a file using a device according to the invention.
- host computer 14
- output device such as monitor or printer 16
- output interface 18
- verification device. 20
- (Dwg.2/2)

PN - DE19961838 A1 20010705 DW200167 H04L9/32 000pp
- WO0146785 A2 20010628 DW200167 G06F1/00 Ger 017pp

OPD - 1999-12-21

PR - DE19991061838 19991221

PA - (SCMM-N) SCM MICROSYSTEMS GMBH

IN - HEINS K W

IC - G06F1/00 ;H04L9/30 ;H04L9/32

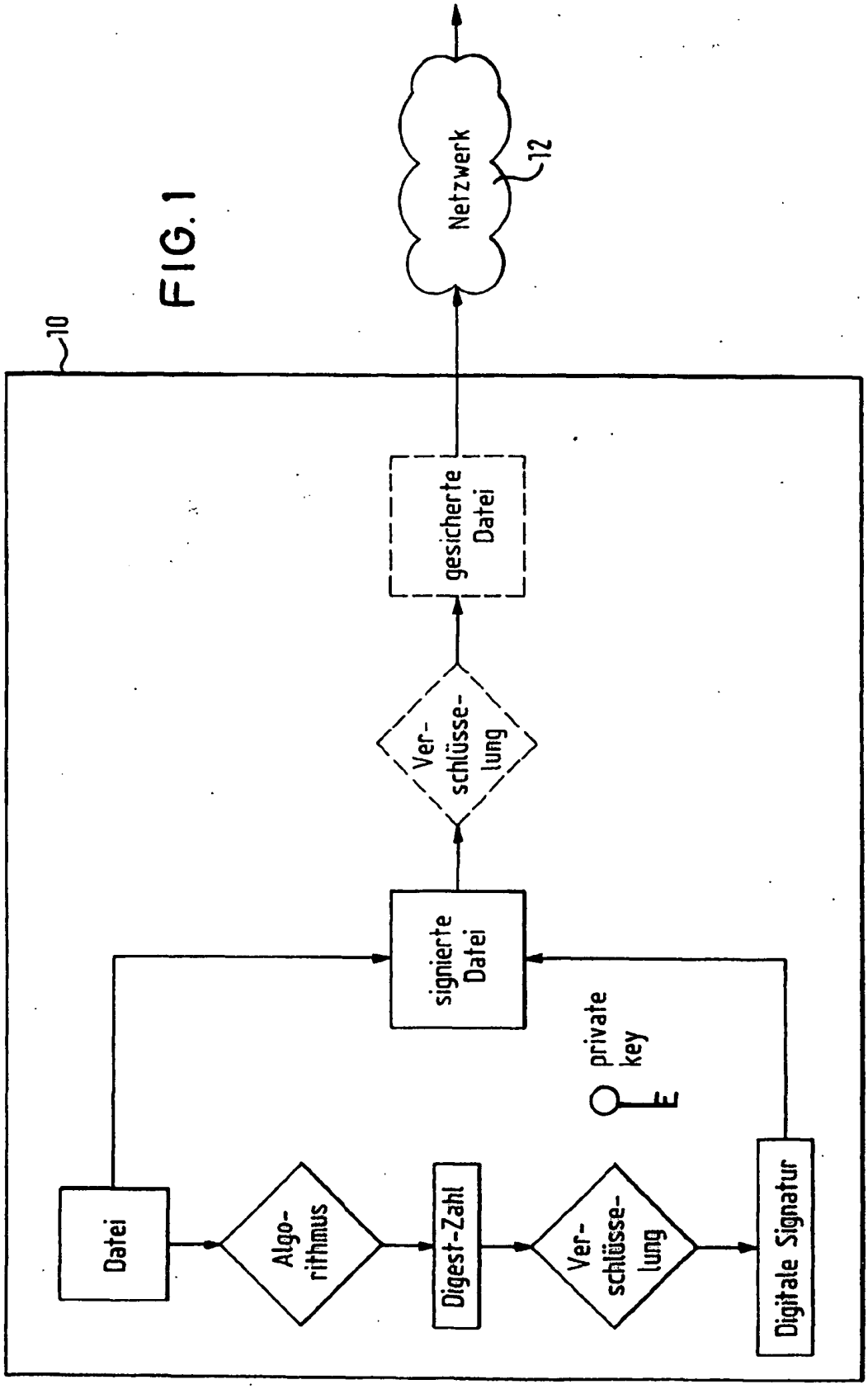
DN - JP SG US

DS - AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR

AN - 2001-596059 [67]

Nummer: DE 199 61 838 A1
Int. Cl.[7]: H 04 L 9/32
Offenlegungstag: 5. Juli 2001

FIG. 1



(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
28. Juni 2001 (28.06.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/46785 A2

(51) Internationale Patentklassifikation[7]: G06F 1/00

(21) Internationales Aktenzeichen: PCT/EP00/13122

(22) Internationales Anmeldedatum:
21. Dezember 2000 (21.12.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
199 61 838.0 21. Dezember 1999 (21.12.1999) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: SCM MICROSYSTEMS GMBH [DE/DE]; Sperl-Ring 4 Hettenshausen, 85276 Pfaffenhofen (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: HEINS, Kersten, W. [DE/DE]; Max-Lehner-Strasse 26, 85354 Freising (DE).

(74) Anwalt: KITZHOFER, Thomas; Prinz & Partner, Manzingerweg 7, 81241 München (DE).

(81) Bestimmungsstaaten *(national)*: JP, SG, US.

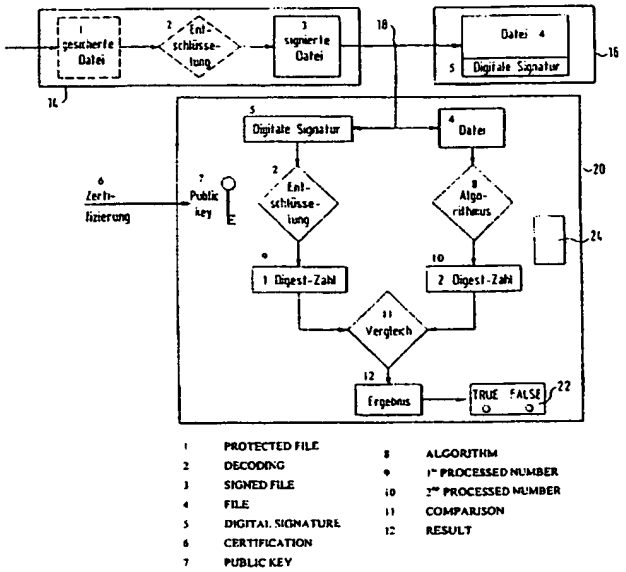
(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Veröffentlicht:
— *Ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts.*

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD AND DEVICE FOR VERIFYING A FILE

(54) Bezeichnung: VERFAHREN UND VORRICHTUNG ZUR ÜBERPRÜFUNG EINER DATEI



(57) Abstract: The invention relates to a method and a device for verifying the authenticity and integrity of a file which has been received, or is to be transmitted from a computer (14) and which is furnished with a digital signature. For the verification process, said method accesses signals which are available at an interface (18) of the computer that is linked to an output device (16) for outputting the file furnished with the digital signature. A device (20) for carrying out the method comprises a circuit and a programme which are used to perform the verification in the device (20), in a manner which is logically separate from the central calculation unit of the computer (14). The device (20) is coupled to an interface (18) of the computer (14) that is linked to an output device (16), in such a way that it detects the signals used for the verification, in order to output the file furnished with the digital signature.

[Fortsetzung auf der nächsten Seite]

WO 01/46785 A2

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Ein Verfahren zur Überprüfung der Authentizität und Integrität einer von einem Rechner (14) empfangenen oder zu versendenden Datei, die mit einer digitalen Signatur versehen ist, greift zur Überprüfung auf Signale zu, die an einer Schnittstelle (18) des Rechners zu einem Ausgabegerät (16) für die Ausgabe der mit der digitalen Signatur versehenen Datei vorliegen. Eine Vorrichtung (20) zur Durchführung des Verfahrens umfasst eine Schaltung und ein Programm, mit denen in der Vorrichtung (20) und logisch getrennt von der zentralen Recheneinheit des Rechners (14) die Überprüfung durchgeführt wird, wobei die Vorrichtung (20) mit einer Schnittstelle (18) des Rechners (14) zu einem Ausgabegerät (16) so gekoppelt ist, dass sie die für die Überprüfung verwendeten Signale zur Ausgabe der mit der digitalen Signatur versehenen Datei erfasst.

Verfahren und Vorrichtung zur Überprüfung einer Datei

Die Erfindung betrifft ein Verfahren zur Überprüfung der Authentizität und Integrität einer von einem Rechner empfangenen oder zu versendenden Datei, die mit einer digitalen Signatur versehen ist. Die Erfindung betrifft ferner eine Vorrichtung zur Durchführung des Verfahrens.

Das Versenden und Empfangen von Dateien auf elektronischem Wege hat mit der fortschreitenden Entwicklung des Internet enorm an Bedeutung gewonnen. Gerade beim Austausch wichtiger Daten (sensitive data), wie er beispielsweise beim Handel über das Internet (e-commerce) stattfindet, besteht der Bedarf der Gewährleistung einer sicheren Datenübertragung. Dies resultiert aus der Tatsache, daß die Informationen, die über das Internet von einem Rechner zu einem entfernten anderen Rechner geschickt werden, eine Reihe von zwischengeschalteten Rechnern und separaten Netzwerken durchlaufen, bevor sie ihr Ziel erreichen. Somit besteht die Gefahr, daß die Übertragung der Daten mittels Dateien vor deren Empfang sowohl durch Übertragungsfehler als auch von dritter Seite auf unerwünschte Weise gestört werden kann.

Insbesondere der Empfänger einer übertragenen Datei hat ein Interesse daran, die Authentizität und die Integrität der empfangenen Datei überprüft zu wissen. Authentizität bedeutet in diesem Zusammenhang die Garantie, daß die Datei tatsächlich von der Person (oder von dem Unternehmen, etc.) stammt, die sich als Absender der Datei ausgibt. Die Integrität einer Datei ist gegeben, wenn deren Inhalt während der Übertragung nicht - vorsätzlich oder zufällig - verändert wurde. Bei bestimmten Anwendungen bestehen seitens des Empfängers die zusätzlichen Forderungen, daß die Vertraulichkeit der übertragenen Daten gewährleistet und/oder das Abstreiten des Versendens der Daten durch den Absender ausgeschlossen ist.

Die Sicherung der Datenübertragung unter Berücksichtigung der oben aufgeführten Aspekte erfolgt auf bekannte Weise unter Verwendung

etablierter Techniken und Standards, die international akzeptiert sind und als Public-Key-Kryptographie bezeichnet werden. Ein wesentlicher Aspekt dieses Verfahrens ist das Versehen einer zu versendenden Datei mit einer digitalen Signatur, die nach dem Empfang der "signierten" Datei auf dem Rechner des Empfängers überprüft wird. Unter einer signierten Datei ist also in diesem Zusammenhang eine Datei samt ihrer zugehörigen digitalen Signatur zu verstehen.

Bei der Überprüfung besteht jedoch die Gefahr, daß bestimmte Viren oder andere bösartige Programme (z.B. spezielle Java-, ActiveX-Anwendungen, etc.) auf dem Rechner des Empfängers die Vorgänge der Überprüfung stören oder so beeinflussen, daß der Empfänger nicht bemerkt, daß die auf dem Bildschirm seines Rechners ausgegebenen Daten nicht mit den abgesandten Daten übereinstimmen. Andererseits ist es auch möglich, daß die Überprüfung der empfangenen Daten korrekt erfolgt und korrekt zu einem positiven Ergebnis führt, daß aber auf dem Bildschirm manipulierte Daten ausgegeben werden, ohne daß eine Warnung an den Empfänger erfolgt.

Das umgekehrte Problem kann auf der Seite des Absenders der Datei auftreten. Wenn beim Signieren einer zu versendenden Datei eine für den Absender nicht erkennbare Störung durch einen Virus oder dergleichen erfolgt, hat der Absender nicht die Möglichkeit, anhand der auf dem Bildschirm angezeigten signierten Datei den Fehler zu erkennen, insbesondere dann, wenn ein Fehler in der digitalen Signatur vorliegt.

Eine Lösung dieser Probleme wäre mit einer komplett eigenständigen Signatur-Architektur möglich, d.h. mit einem speziellen System, das abgeschirmt von der Umgebung nur zur Überprüfung von Dateien vorgesehen ist. Da ein solches System jedoch einen eigenen Prozessor und eigene Peripheriegeräte wie Tastatur, Bildschirm, etc. benötigen würde, ist es für den vorgesehenen Zweck zu kostspielig.

Aus der US 5 406 624 ist eine Sicherheitsvorrichtung für einen Rechner bekannt, mit der sicherheitsrelevante Daten von dem möglicherweise mit Viren oder dergleichen infizierten Rechner ferngehalten werden. Die Vorrichtung dient ferner dazu, Vorgänge wie das Erzeugen von Schlüsseln und das Schreiben der Schlüssel auf Smart-Cards unabhängig von dem Rechner durchzuführen. Dazu ist der Rechner von seinen Peripheriegeräten isoliert,

indem diese nicht direkt sondern über die zwischengeschaltete Sicherheitsvorrichtung mit dem Rechner verbunden sind. Zur Durchführung der sicherheitsrelevanten Vorgänge übernimmt die Vorrichtung die Kontrolle über die Peripheriegeräte und führt selbständig die erforderlichen Operationen wie etwa das Lesen oder Beschreiben einer Smart-Card durch. Die Sicherheitsvorrichtung ist jedoch nicht dafür geeignet, eine auf einem Ausgabegerät des Rechners ausgegebene, online empfangene oder zu versendende Datei auf deren Authentizität und Integrität zu überprüfen. Nachteilig an dieser Vorrichtung ist weiterhin, daß zu deren Aktivierung spezielle Befehle oder eine separate Switch-Box benötigt werden. Außerdem ist die Sicherheitsvorrichtung sehr aufwendig und damit teuer, da sie für die Durchführung komplexer Vorgänge, wie sie das Lesen und Beschreiben einer Smart-Card darstellen, ausgelegt ist. Zudem muß eine komplette, separate Bildschirmansteuerung in der Sicherheitsvorrichtung vorhanden sein.

Es ist daher Aufgabe der Erfindung, eine Möglichkeit zur Überprüfung einer empfangenen oder versandfertigen signierten Datei bereitzustellen, die eine möglichst sichere Information bezüglich der Authentizität und Integrität der auf einem Ausgabegerät eines Rechners ausgegebenen Datei liefert.

Gelöst wird diese Aufgabe durch ein Verfahren der eingangs genannten Art, bei dem zur Überprüfung auf Signale zugegriffen wird, die an einer Schnittstelle des Rechners zu einem Ausgabegerät für die Ausgabe der mit der digitalen Signatur versehenen Datei vorliegen. Dies ermöglicht eine Überprüfung der Daten, wie sie auf dem Ausgabegerät des Rechners ausgegeben und vom Benutzer wahrgenommen werden. Die Erfindung beruht auf der Erkenntnis, daß die Signale, die an ein Ausgabegerät des Rechners abgegeben werden, durch Viren oder dergleichen nicht angegriffen werden können, da das Ausgabegerät eine passive Einheit darstellt, die die Daten nicht mehr bearbeitet. Somit kann der Betrachter der signierten Datei darüber informiert werden, ob die auf dem Ausgabegerät ausgegebene Datei und die digitale Signatur zusammenpassen. Bei positivem Ergebnis ist auf diese Weise sichergestellt, daß die zur Überprüfung herangezogenen Daten (Datei und digitale Signatur) nicht nachträglich auf dem Rechner des Empfängers oder im Netzwerk manipuliert wurden.

Da vorgesehen ist, das erfindungsgemäße Verfahren in einer von der zentralen Recheneinheit (CPU) des Rechners logisch getrennten Vorrichtung durchzuführen, kann die Überprüfung der Datei nicht durch Viren oder dergleichen gestört werden, die möglicherweise auf die im Rechner stattfindende Datenverarbeitung einwirken.

Die Rekonstruktion der auf dem Ausgabegerät ausgegebenen Datei und deren digitaler Signatur aus den Signalen, die an der Schnittstelle vorliegen, ermöglicht eine verhältnismäßig unkomplizierte Überprüfung der ausgegebenen signierten Datei unter Verwendung bekannter Verfahren.

Vorzugsweise umfaßt das erfindungsgemäße Verfahren die Entschlüsselung der digitalen Signatur der rekonstruierten signierten Datei, wobei durch die Entschlüsselung eine erste Digest-Zahl erzeugt wird. Diese erste Digest-Zahl kann dann auf einfache Weise mit einer zweiten Digest-Zahl verglichen werden, die aus der rekonstruierten Datei bestimmt wird. Das Ergebnis dieses Vergleichs gibt einen sicheren Aufschluß über die Authentizität und Integrität der ausgegebenen Datei, vorausgesetzt, daß der verwendete Schlüssel tatsächlich zum Absender gehört. Diese Zuordnung zwischen öffentlichem Schlüssel und Absender wird aber üblicherweise über eine unabhängige Zertifizierungsstelle sichergestellt. Zudem kann sich bei positivem Ergebnis des Vergleichs, wenn es sich bei der Datei um eine empfangene Datei handelt, der Empfänger sicher sein, daß die Datei vom Absender auch tatsächlich abgeschickt wurde. Somit kann z.B. der Absender ein in der Datei enthaltenes Angebot nicht gegenstandslos machen, indem er bestreitet, diese Datei jemals abgeschickt zu haben.

Gemäß einer Weiterbildung des Verfahrens ist vorgesehen, auch den Erstellungszeitpunkts der mit der digitalen Signatur versehenen Datei zu überprüfen. So kann z.B. bei empfangenen Dateien eine gesicherte Auskunft über die Gültigkeit eines in der signierten Datei enthaltenen, zeitlich befristeten Angebots zum Zeitpunkt des Empfangs gegeben werden.

Besonders geeignet ist das erfindungsgemäße Verfahren für Dateien, die online aus einem Netzwerk empfangen wurden bzw. online über ein Netzwerk versendet werden, da solche Dateien einem erhöhten Risiko der fehlerhaften Übertragung oder Manipulation unterliegen.

Schließlich erweist es sich als vorteilhaft, wenigstens einen Teil des Verfahrens mittels einer Chipkarte durchzuführen. Wenn der Rechner beispielsweise mit einem Smart-Card-Terminal ausgestattet ist, können mit einer entsprechenden Smart-Card sowohl im Zusammenhang mit dem erfindungsgemäßen Verfahren erforderliche Entschlüsselungsvorgänge als auch Überprüfungen von Schlüsseln unterstützt werden.

Die Erfindung sieht auch eine Vorrichtung zur Durchführung des Verfahrens vor, die eine Schaltung und ein Programm umfaßt, mit denen in der Vorrichtung und logisch getrennt von der zentralen Recheneinheit des Rechners die Überprüfung durchgeführt wird, wobei die Vorrichtung mit einer Schnittstelle des Rechners zu einem Ausgabegerät so gekoppelt ist, daß sie die für die Überprüfung verwendeten Signale zur Ausgabe der mit der digitalen Signatur versehenen Datei erfaßt. Mit der erfindungsgemäßen Vorrichtung können so auf einfache Weise die für die Ausgabe der signierten Datei vorgesehenen, nicht angreifbaren Signale abgetastet und ausgewertet werden. Auch die Überprüfung der Datei kann aufgrund der Trennung der Vorrichtung von der Datenverarbeitung des Rechners nicht gestört werden.

Vorzugsweise ist die Vorrichtung an die Schnittstelle des Rechners zu einem Bildschirm gekoppelt. So erhält beispielsweise der Empfänger einer Datei die gesicherte Information, ob die empfangene Datei in der Form, wie sie am Bildschirm angezeigt wird, tatsächlich vom angegebenen Absender stammt und störungsfrei übertragen wurde. Die Vorrichtung kann jedoch auch an die Schnittstelle des Rechners zu einem Drucker gekoppelt sein.

Für eine kostengüstige Herstellung der Vorrichtung ist es vorteilhaft, daß die Vorrichtung einen ASIC (application-specific integrated circuit) umfaßt, der die für die Überprüfung notwendige Schaltung beherbergt. Der ASIC kann auch einen Mikroprozessor aufweisen, der programmgesteuert arbeitet.

Eine Flexibilität in bezug auf die Auswahl des Rechners, an dem die Vorrichtung eingesetzt werden soll, wird dadurch erreicht, daß die Vorrichtung für die nachträgliche Ausstattung des Rechners geeignet ist, d.h. als sogenanntes Add-On-System ausgeführt ist. Die Vorrichtung kann auf einfache Weise an dem gewünschten Rechner eingerichtet und bei Bedarf

wieder deinstalliert werden, um einen anderen Rechner mit der Vorrichtung auszustatten.

Die Vorrichtung kann intern auf der Basisplatine (motherboard) oder auf einer Einsteckkarte des Rechners angeordnet sein. Sie kann aber auch in einem externen Gerät verwirklicht sein, das an den Rechner angeschlossen ist. So ist es beispielsweise möglich, die Vorrichtung in ein Chipkarten-Terminal, z.B. ein Smart-Card-Lese-/Schreibgerät zu integrieren. Vorzugsweise weist die Vorrichtung eine dem Chipkarten-Terminal zugeordnete Chipkarte auf, die so mit der restlichen Vorrichtung verknüpft ist, daß sie einen Entschlüsselungsvorgang zumindest teilweise durchführt oder Daten für einen Entschlüsselungsvorgang bereitstellt. Somit besteht die Möglichkeit, wenigstens einen Teil des erfindungsgemäßen Verfahrens mit Hilfe oder direkt von einem Mikroprozessor der Smart-Card durchführen zu lassen. Mit dem Terminal können aber auch andere, auf das erfindungsgemäße Verfahren bezogene Funktionen ausgeführt werden.

Um den Benutzer einfach und unkompliziert über das Ergebnis der Dateiüberprüfung zu informieren, umfaßt die Vorrichtung eine TRUE/FALSE-Anzeige.

Eine bevorzugte Ausführungsform der erfindungsgemäßen Vorrichtung umfaßt eine Echtzeituhr, mit deren Hilfe das Alter einer signierten Datei bestimmt werden kann. Dies kann z.B. für die Überprüfung erforderlich sein, ob ein in der Datei enthaltenes Angebot noch gültig ist.

Falls die Vorrichtung an wechselnden Orten aufgestellt werden soll, kann die Kopplung der Vorrichtung an die Schnittstelle des Rechners drahtlos erfolgen. Damit ist die Auswahl der Standorte nicht durch die Länge eines Kabels oder dessen unerwünschte Sichtbarkeit beeinträchtigt.

Weitere Merkmale und Vorteile der Erfindung ergeben sich aus der nachfolgenden beispielhaften Beschreibung unter Bezugnahme auf die Zeichnung. In dieser zeigen:

Fig. 1 ein schematisches Flußdiagramm für die Verarbeitung einer zu versendenden Datei; und

Fig. 2 ein schematisches Flußdiagramm für die Überprüfung einer empfangenen Datei mit der erfindungsgemäßen Vorrichtung, die nach dem erfindungsgemäßen Verfahren arbeitet.

Im folgenden werden das erfindungsgemäße Verfahren und die dafür vorgesehene erfindungsgemäße Vorrichtung am Beispiel der Überprüfung einer empfangenen Datei beschrieben. Es ist jedoch genauso möglich, das Verfahren und die Vorrichtung auf der Seite des Empfängers zur Überprüfung einer versandfertigen Datei, die an der Schnittstelle zum Netzwerk anliegt, zu verwenden.

In Figur 1 sind die Vorgänge dargestellt, der gemäß dem Konzept der Public-Key-Kryptographie üblicherweise auf einem Rechner 10 des Absenders vor dem Versenden einer Datei ablaufen. Aus der von dem Absender erstellten Datei, die zu einem Empfänger geschickt werden soll, wird mittels eines vorgegebenen mathematischen Algorithmus eine sogenannte Digest-Zahl berechnet. Eine Digest-Zahl hat eine bestimmte Länge und ist für die jeweilige Datei spezifisch, d.h. die kleinste Änderung in der Datei würde zu einem unterschiedlichen Wert führen. Andererseits kann jedoch aus der Digest-Zahl niemals die ursprüngliche Datei erhalten werden. Die Digest-Zahl der Datei wird mittels eines privaten Schlüssels (private key) des Absenders verschlüsselt, der nur dem Absender bekannt ist. Das Ergebnis dieser Verschlüsselung wird als digitale Signatur der Datei bezeichnet. Die digitale Signatur wird an die zu versendende Datei angehängt. Die mit der digitalen Signatur versehene (signierte) Datei kann nun entweder gleich über ein Netzwerk 12 an den Empfänger verschickt oder, falls die Daten vertraulich sind, vorher verschlüsselt werden.

Die optionale Verschlüsselung der signierten Datei erfolgt üblicherweise mittels eines zufällig erzeugten einmaligen Schlüssels (one time key). Der einmalige Schlüssel selbst wird wiederum mit einem öffentlichen Schlüssel (public key) verschlüsselt und anschließend an die signierte, verschlüsselte Datei angehängt. Beide zusammen werden schließlich als "gesicherte Datei" an den Empfänger verschickt.

Figur 2 zeigt die Vorgänge, die zur Überprüfung der empfangenen Datei auf der Seite des Empfängers durchgeführt werden. Die von einem Rechner 14 empfangene Datei wird als gesicherte oder lediglich signierte Datei

erkannt. Im ersten Fall wird die gesicherte Datei zunächst auf dem Rechner 14 mittels eines privaten Schlüssels des Empfängers entschlüsselt, wodurch eine signierte, aber noch verschlüsselte Datei und ein einmaliger Schlüssel erhalten werden. Mit dem einmaligen Schlüssel kann nun die signierte, verschlüsselte Datei entschlüsselt werden. Die daraus resultierende signierte Datei wird anschließend so weiterverarbeitet wie eine unverschlüsselt empfangene Datei, die mit einer Signatur versehen ist.

Um die signierte Datei für den Empfänger sichtbar zu machen, wird sie auf einem Ausgabegerät 16 ausgegeben, das über eine Schnittstelle 18 an den Rechner 14 angeschlossen ist. Das Ausgabegerät 16 ist im Regelfall ein Bildschirm, es kann jedoch beispielsweise auch ein Drucker o.ä. vorgesehen sein. Die vom Rechner 14 an das Ausgabegerät 16 abgegebenen Signale zur Anzeige der signierten Datei sind logisch von der zentralen Recheneinheit des Rechners 14 getrennt, d.h. diese Signale können nicht durch Programme beeinflußt werden, die auf dem Rechner 14 ablaufen. Somit sind diese Signale auch nicht durch Viren oder dergleichen angreifbar.

An der Schnittstelle 18 ist neben dem Ausgabegerät 16 auch eine Vorrichtung 20 angeschlossen, die auf die für das Ausgabegerät 16 bestimmten Signale zugreifen kann. Normalerweise handelt es sich bei einer Schnittstelle 18 zu einem Bildschirm um eine analoge Schnittstelle. Bei modernen Bildschirmen, die die anzuzeigenden Daten selbst in analoge Signale umwandeln, ist dementsprechend eine digitale Schnittstelle vorgesehen. Der Einfachheit halber werden die in diesem Fall an der Schnittstelle vorliegenden Daten ebenfalls als "Signale" bezeichnet. Sowohl die Verbindung des Ausgabegeräts 16 als auch der Vorrichtung 20 mit der Schnittstelle 18 des Rechners 14 kann drahtlos erfolgen, z.B. mittels aufeinander abgestimmter Infrarot-Schnittstellen an den beteiligten Geräten.

Die Vorrichtung 20 weist eine elektronische Schaltung, die in einem ASIC untergebracht sein kann, und ein geeignetes Programm zur Überprüfung der signierten Datei auf. Da die Vorrichtung 20 logisch getrennt von der zentralen Recheneinheit des Rechners 14 ist, können keine Viren oder dergleichen, die sich beispielsweise im Hauptspeicher des Rechners 14 befinden und die Datenverarbeitung auf unerwünschte Weise beeinflussen,

die Überprüfung der signierten Datei stören.

Die Überprüfung der signierten Datei in der Vorrichtung 20 wird im folgenden für den Fall eines Bildschirms als Ausgabegerät 16 beschrieben: Die an der Schnittstelle 18 vorliegenden Signale werden von der Vorrichtung 20 abgetastet und ausgewertet. Dadurch kann das auf dem Bildschirm ausgegebene Bild rekonstruiert werden, und die darin "angezeigte" Datei samt zugehöriger digitaler Signatur wird ausfindig gemacht. Die digitale Signatur wird mittels eines öffentlichen Schlüssels entschlüsselt, der vom Absender öffentlich zugänglich gemacht wurde und auf den privaten Schlüssel abgestimmt ist, mit dem die vom Absender aus der ursprünglichen Datei erzeugte Digest-Zahl verschlüsselt wurde. Der öffentliche Schlüssel ist von einer unabhängigen Zertifizierungsstelle zertifiziert. Das Ergebnis dieser Entschlüsselung ist eine erste Digest-Zahl. Eine zweite Digest-Zahl wird aus der Datei selbst berechnet. Dazu wird der gleiche mathematische Algorithmus verwendet, der auf dem Rechner 10 des Absenders die ursprüngliche Digest-Zahl erzeugt hat. Die für diesen Vorgang notwendigen Informationen über den mathematischen Algorithmus sind mit der digitalen Signatur verschickt worden. Die beiden Digest-Zahlen werden schließlich miteinander verglichen und das Ergebnis wird über eine TRUE/FALSE-Ausgabeeinrichtung 22 der Vorrichtung 20 ausgegeben. Das Ergebnis kann beispielsweise bei übereinstimmenden Digest-Zahlen (TRUE) durch eine grüne Leuchtdiode und bei nicht übereinstimmenden Digest-Zahlen (FALSE) durch eine rote Leuchtdiode angezeigt werden.

Stimmen die beiden Digest-Zahlen überein, wurde die Datei nach dem Signieren durch den Absender nicht mehr verändert. Außerdem hat der Empfänger hat Gewißheit über die Identität des Absenders, da durch die Zertifizierung des öffentlichen Schlüssels dessen Zugehörigkeit zu dem Absender sichergestellt ist. Da alleine der Absender Zugriff auf den privaten Schlüssel hat, der zum Signieren der Datei benutzt wurde, kann der Absender auch nicht abstreiten, daß er die Datei verschickt hat. Bei Nichtübereinstimmung der beiden Digest-Zahlen muß davon ausgegangen werden, daß die Datei entweder nicht korrekt übertragen oder manipuliert wurde oder daß die Signatur mit einem privaten Schlüssel erzeugt wurde, der nicht zu dem für die Entschlüsselung der digitalen Signatur benutzten öffentlichen Schlüssel paßt.

Eine bevorzugte Ausführungsform der Vorrichtung 20 umfaßt zusätzlich eine Echtzeituhr 24 zur gesicherten Bestimmung des Alters der Datei, z.B. der Zeitdifferenz zwischen Empfangs- und Erstellungszeitpunkt der Datei. Dazu wird die Datei vor dem Verschicken neben der digitalen Signatur mit einer Angabe über den Erstellungs- oder Absendezeitpunkt oder den Gültigkeitszeitraum versehen, die als Zeitstempel bezeichnet werden kann. In der Vorrichtung 20 kann nun anhand eines Vergleichs dieser Zeitangabe mit der aktuellen Zeit ermittelt werden, ob z.B. ein in der Datei enthaltenes, zeitlich befristetes Angebot noch gültig ist. Diese Überprüfung wird dann bei der Anzeige des Ergebnisses der Dateiüberprüfung mit berücksichtigt.

Die Vorrichtung 20 ist als Add-On-System konzipiert, d.h. ein Rechner kann nachträglich mit der Vorrichtung 20 ausgestattet werden. Dabei kann die Vorrichtung 20 sowohl intern im Rechner 14 auf der Basisplatine oder auf einer Einsteckkarte angeordnet sein. Gemäß einer weiteren Ausführungsform ist die die Vorrichtung 20 in ein Smart-Card-Terminal integriert. Mit Hilfe des Smart-Card-Terminals und entsprechender Smart-Card kann gleichzeitig die Zertifizierung des öffentlichen Schlüssels überprüft werden, der für die Entschlüsselung der digitalen Signatur benötigt wird. Weiterhin kann mit Hilfe einer geeigneten Smart-Card die Entschlüsselung der digitalen Signatur oder gegebenenfalls der gesicherten Datei unterstützt werden. Die Smart-Card enthält beispielsweise einen für die jeweilige Entschlüsselung notwendigen Schlüssel und/oder ein Entschlüsselungsprogramm. Ein Teil oder die gesamte Entschlüsselung kann von einem Mikroprozessor der Smart-Card durchgeführt oder gesteuert werden.

Patentansprüche

1. Verfahren zur Überprüfung der Authentizität und Integrität einer von einem Rechner (10; 14) empfangenen oder zu versendenden Datei, die mit einer digitalen Signatur versehen ist, dadurch gekennzeichnet, daß zur Überprüfung auf Signale zugegriffen wird, die an einer Schnittstelle (18) des Rechners (10; 14) zu einem Ausgabegerät (16) für die Ausgabe der mit der digitalen Signatur versehenen Datei vorliegen.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß das Verfahren in einer von der zentralen Recheneinheit des Rechners (10; 14) logisch getrennten Vorrichtung (20) durchgeführt wird.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß das Verfahren die Rekonstruktion der auf dem Ausgabegerät (16) ausgegebenen, mit der digitalen Signatur versehenen Datei aus den Signalen umfaßt, die an der Schnittstelle vorliegen.

4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, daß das Verfahren die Entschlüsselung der digitalen Signatur der rekonstruierten signierten Datei umfaßt, wobei durch die Entschlüsselung eine erste Digest-Zahl erzeugt wird.

5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß das Verfahren die Bestimmung einer zweiten Digest-Zahl aus der rekonstruierten Datei und das Vergleichen der ersten Digest-Zahl mit der zweiten Digest-Zahl umfaßt.

6. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß das Verfahren die Überprüfung des Erstellungszeitpunkts der mit der digitalen Signatur versehenen Datei umfaßt.

7. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die mit der digitalen Signatur versehene Datei online aus einem Netzwerk empfangen wurde bzw. online über ein Netzwerk versendet wird.

8. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß wenigstens ein Teil des Verfahrens mittels einer Chipkarte durchgeführt wird.

9. Vorrichtung zur Durchführung des Verfahrens nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Vorrichtung (20) eine Schaltung und ein Programm umfaßt, mit denen in der Vorrichtung (20) und logisch getrennt von der zentralen Recheneinheit des Rechners (10; 14) die Überprüfung durchgeführt wird, und die Vorrichtung (20) mit einer Schnittstelle (18) des Rechners (10; 14) zu einem Ausgabegerät (16) so gekoppelt ist, daß sie die für die Überprüfung verwendeten Signale zur Ausgabe der mit der digitalen Signatur versehenen Datei erfaßt.

10. Vorrichtung nach Anspruch 9, dadurch gekennzeichnet, daß die Vorrichtung (20) an die Schnittstelle (18) des Rechners (10; 14) zu einem Bildschirm gekoppelt ist.

11. Vorrichtung nach Anspruch 9, dadurch gekennzeichnet, daß die Vorrichtung (20) an die Schnittstelle (18) des Rechners (10; 14) zu einem Drucker gekoppelt ist.

12. Vorrichtung nach einem der Ansprüche 9 bis 11, dadurch gekennzeichnet, daß die Vorrichtung (20) einen ASIC umfaßt.

13. Vorrichtung nach einem der Ansprüche 9 bis 12, dadurch gekennzeichnet, daß die Vorrichtung (20) für die nachträgliche Ausstattung des Rechners (10; 14) geeignet ist.

14. Vorrichtung nach einem der Ansprüche 9 bis 13, dadurch gekennzeichnet, daß die Vorrichtung (20) auf der Basisplatine des Rechners (10; 14) angeordnet ist.

15. Vorrichtung nach einem der Ansprüche 9 bis 13, dadurch gekennzeichnet, daß die Vorrichtung (20) auf einer Einsteckkarte des Rechners (10; 14) angeordnet ist.

16. Vorrichtung nach einem der Ansprüche 9 bis 13, dadurch gekenn-

zeichnet, daß die Vorrichtung (20) in ein Chipkarten-Terminal integriert ist.

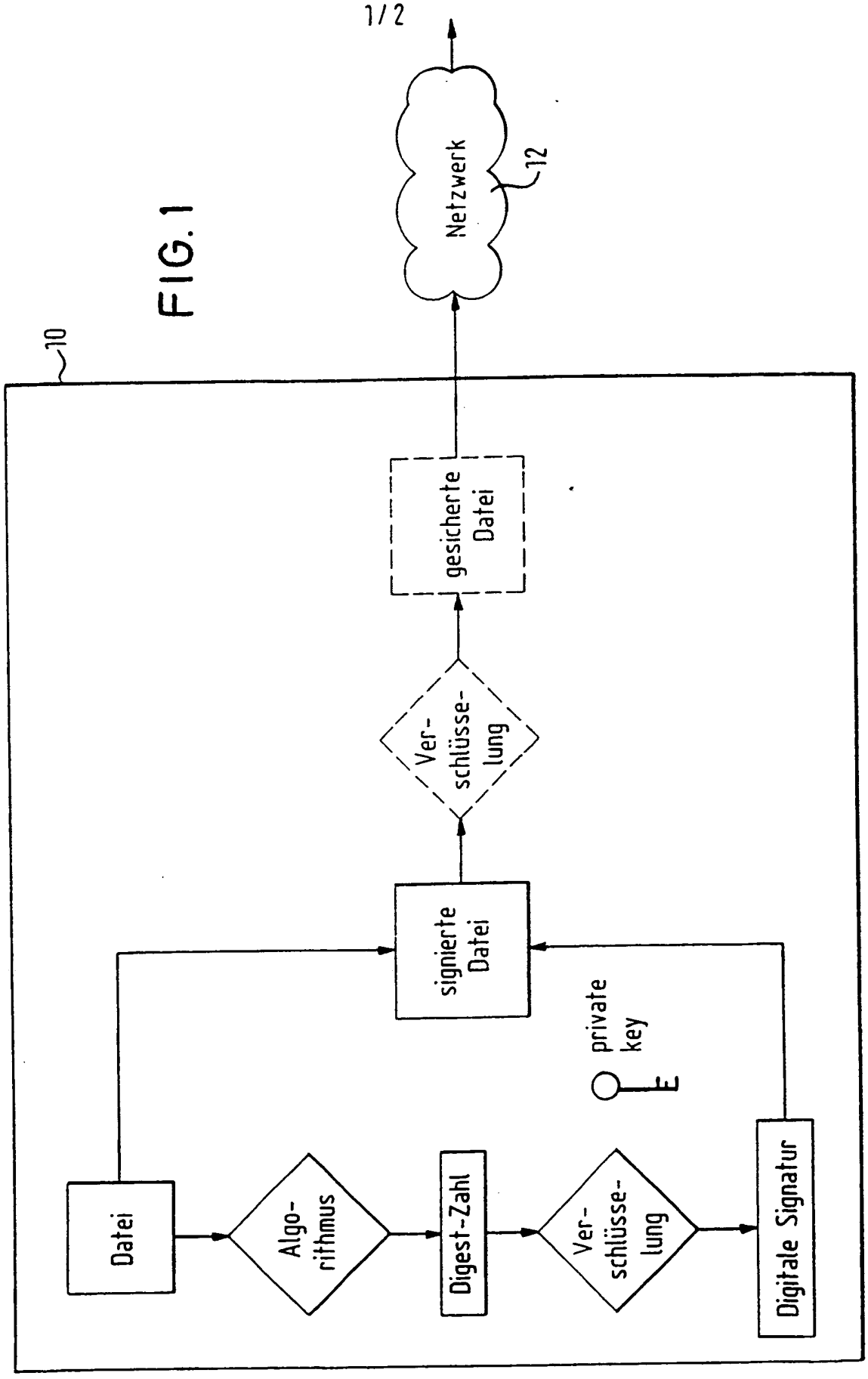
17. Vorrichtung nach Anspruch 16, dadurch gekennzeichnet, daß die Vorrichtung (20) eine dem Chipkarten-Terminal zugeordnete Chipkarte aufweist, die so mit der restlichen Vorrichtung verknüpft ist, daß sie einen Entschlüsselungsvorgang zumindest teilweise durchführt oder Daten für einen Entschlüsselungsvorgang bereitstellt.

18. Vorrichtung nach einem der Ansprüche 9 bis 17, dadurch gekennzeichnet, daß die Vorrichtung (20) eine TRUE/FALSE-Anzeigeeinrichtung umfaßt.

19. Vorrichtung nach einem der Ansprüche 9 bis 18, dadurch gekennzeichnet, daß die Vorrichtung (20) eine Echtzeituhr (22) umfaßt.

20. Vorrichtung nach einem der Ansprüche 9 bis 19, dadurch gekennzeichnet, daß die Kopplung der Vorrichtung (20) an die Schnittstelle (18) des Rechners (10; 14) drahtlos erfolgt.

FIG. 1


Netzwerk
12
10
gesicherte Datei
Ver-schlüsse-lung
signierte Datei
private key
Datei
Algo-rithmus
Digest-Zahl
Ver-schlüsse-lung
Digitale Signatur

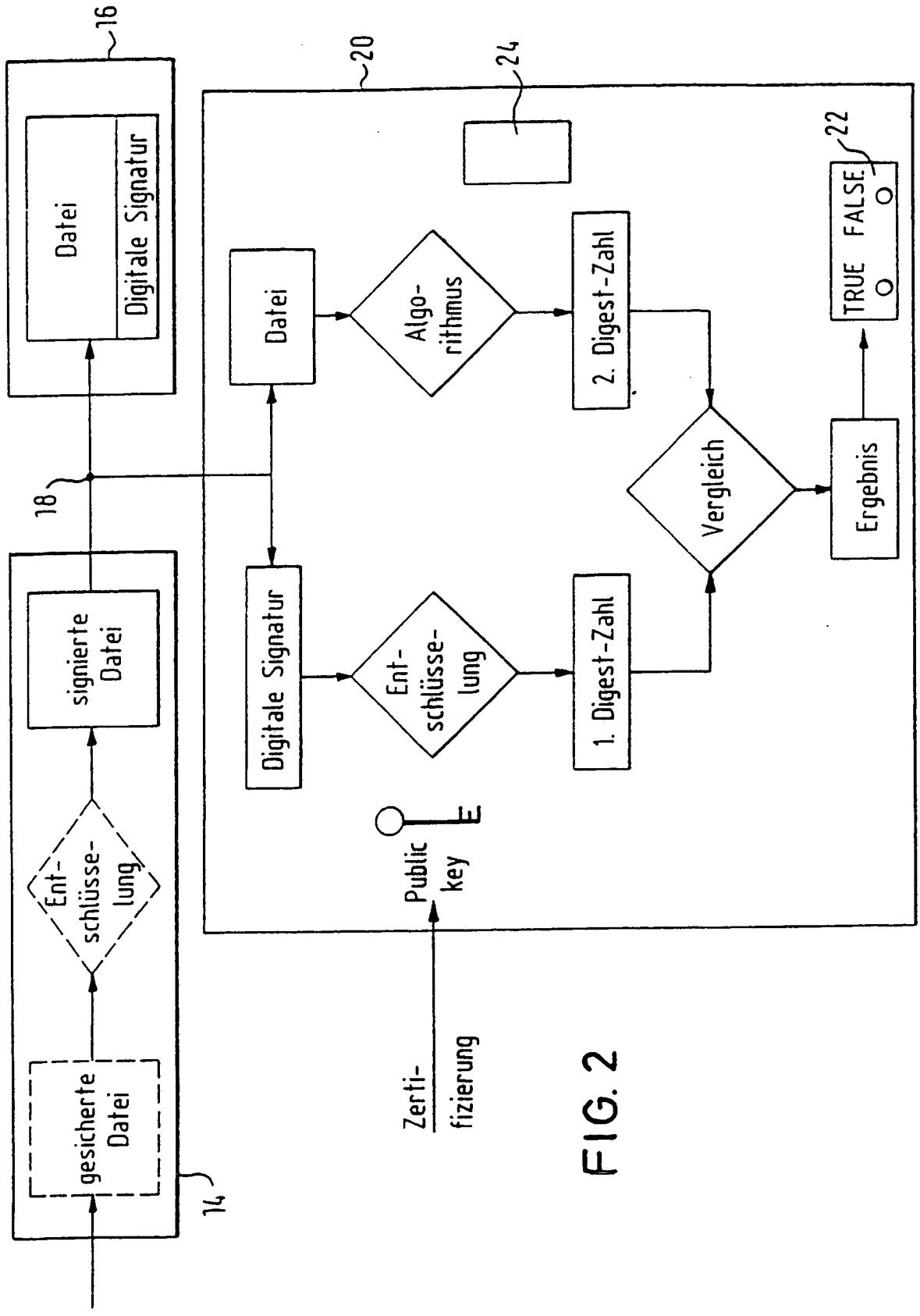

16
Datei
Digitale Signatur
20
24
22
TRUE FALSE
Datei
Algo-rithmus
2. Digest-Zahl
18
Vergleich
Ergebnis
Digitale Signatur
Ent-schlüsse-lung
1. Digest-Zahl
signierte Datei
Ent-schlüsse-lung
Public key
gesicherte Datei
14
Zerti-fizierung

FIG. 2

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
28. Juni 2001 (28.06.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/46785 A3

(51) Internationale Patentklassifikation⁷: G06F 1/00

(21) Internationales Aktenzeichen: PCT/EP00/13122

(22) Internationales Anmeldedatum:
21. Dezember 2000 (21.12.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
199 61 838.0 21. Dezember 1999 (21.12.1999) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: SCM MICROSYSTEMS GMBH [DE/DE]; Sperl-Ring 4 Hettenshausen, 85276 Pfaffenhofen (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: HEINS, Kersten, W. [DE/DE]; Max-Lehner-Strasse 26, 85354 Freising (DE).

(74) Anwalt: KITZHOFER, Thomas; Prinz & Partner, Manzingerweg 7, 81241 München (DE).

(81) Bestimmungsstaaten *(national)*: JP, SG, US.

(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

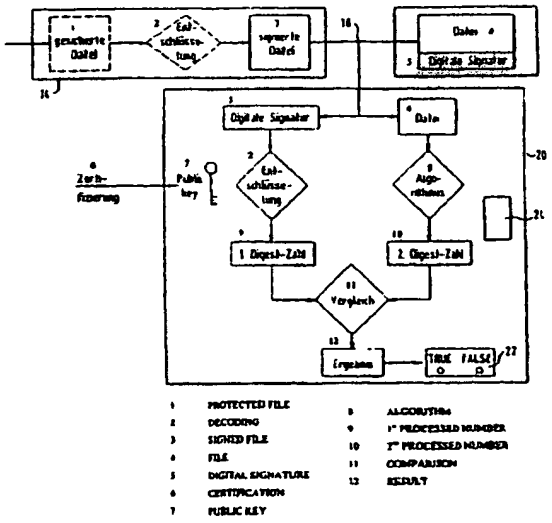
Veröffentlicht:
mit internationalem Recherchenbericht

(88) Veröffentlichungsdatum des internationalen Recherchenberichts: 6. Dezember 2001

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(54) Title: METHOD AND DEVICE FOR VERIFYING A FILE

(54) Bezeichnung: VERFAHREN UND VORRICHTUNG ZUR ÜBERPRÜFUNG EINER DATEI



(57) Abstract: The invention relates to a method and a device for verifying the authenticity and integrity of a file which has been received, or is to be transmitted from a computer (14) and which is furnished with a digital signature. For the verification process, said method accesses signals which are available at an interface (18) of the computer that is linked to an output device (16) for outputting the file furnished with the digital signature. A device (20) for carrying out the method comprises a circuit and a programme which are used to perform the verification in the device (20), in a manner which is logically separate from the central calculation unit of the computer (14). The device (20) is coupled to an interface (18) of the computer (14) that is linked to an output device (16), in such a way that it detects the signals used for the verification, in order to output the file furnished with the digital signature.

[Fortsetzung auf der nächsten Seite]

WO 01/46785 A3

(57) **Zusammenfassung:** Ein Verfahren zur Überprüfung der Authentizität und Integrität einer von einem Rechner (14) empfangenen oder zu versendenden Datei, die mit einer digitalen Signatur versehen ist, greift zur Überprüfung auf Signale zu, die an einer Schnittstelle (18) des Rechners zu einem Ausgabegerät (16) für die Ausgabe der mit der digitalen Signatur versehenen Datei vorliegen. Eine Vorrichtung (20) zur Durchführung des Verfahrens umfasst eine Schaltung und ein Programm, mit denen in der Vorrichtung (20) und logisch getrennt von der zentralen Recheneinheit des Rechners (14) die Überprüfung durchgeführt wird, wobei die Vorrichtung (20) mit einer Schnittstelle (18) des Rechners (14) zu einem Ausgabegerät (16) so gekoppelt ist, dass sie die für die Überprüfung verwendeten Signale zur Ausgabe der mit der digitalen Signatur versehenen Datei erfasst.

INTERNATIONAL SEARCH REPORT

Int ational Application No
PC1/EP 00/13122

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 587 375 A (ALGORITHMIC RES LTD) 16 March 1994 (1994-03-16) column 1, line 11 -column 3, line 28 figure 1 ---	1-3,9-12
A	US 5 778 071 A (AMORUSO VICTOR P ET AL) 7 July 1998 (1998-07-07) column 12, line 14 -column 13, line 3 ---	1-4,7-9
A	EP 0 722 151 A (XEROX CORP) 17 July 1996 (1996-07-17) abstract; figure 2 -----	1,9

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 July 2001	23/07/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Sigolo, A

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 00/13122

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0587375 A	16-03-1994	IL 103062 A	04-08-1996
		GB 2267986 A,B	22-12-1993
		SG 43927 A	14-11-1997
		US 5406624 A	11-04-1995
US 5778071 A	07-07-1998	US 5546463 A	13-08-1996
		AU 726397 B	09-11-2000
		AU 4147097 A	06-03-1998
		EP 0916210 A	19-05-1999
		WO 9807255 A	19-02-1998
		US 5878142 A	02-03-1999
EP 0722151 A	17-07-1996	BR 9600053 A	21-01-1998
		JP 8290639 A	05-11-1996
		US 5720012 A	17-02-1998

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 00/13122

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G06F1/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data, PAJ, INSPEC

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP 0 587 375 A (ALGORITHMIC RES LTD) 16. März 1994 (1994-03-16) Spalte 1, Zeile 11 -Spalte 3, Zeile 28 Abbildung 1	1-3,9-12
A	US 5 778 071 A (AMORUSO VICTOR P ET AL) 7. Juli 1998 (1998-07-07) Spalte 12, Zeile 14 -Spalte 13, Zeile 3	1-4,7-9
A	EP 0 722 151 A (XEROX CORP) 17. Juli 1996 (1996-07-17) Zusammenfassung; Abbildung 2	1,9

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
17. Juli 2001	23/07/2001

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Sigolo, A

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP 00/13122

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 0587375 A	16-03-1994	IL 103062 A	04-08-1996
		GB 2267986 A,B	22-12-1993
		SG 43927 A	14-11-1997
		US 5406624 A	11-04-1995
US 5778071 A	07-07-1998	US 5546463 A	13-08-1996
		AU 726397 B	09-11-2000
		AU 4147097 A	06-03-1998
		EP 0916210 A	19-05-1999
		WO 9807255 A	19-02-1998
		US 5878142 A	02-03-1999
EP 0722151 A	17-07-1996	BR 9600053 A	21-01-1998
		JP 8290639 A	05-11-1996
		US 5720012 A	17-02-1998